5 FAH-2 H-860
ANTI-VIRUS PROGRAM

(TL:TEL-1;   07-01-1998))

5 FAH-2 H-861 POLICY

(TL:TEL-1;   07-01-1998)
(Uniform State/USAID/USIA)

a. According to 12 FAM 643.2-9 all systems connected to Department networks must be protected with virus detection and prevention programs. IRM/OPS/ITI/SI/IIB (Systems Integrity Division, Information Integrity Branch) provides anti-virus software and documentation to all bureaus and field posts free of charge. The software includes initial and updated definition files for IBM compatible and Macintosh systems operating the full range of Microsoft environments. The Setup and Installation Procedures Handbook answers procedural questions about installation. Contact IRM/OPS/ITI/SI/IIB at (202) 647-4555 for more information.

b. The anti-virus material may be mass-produced and provided to all U.S. Government employees and contractors to the extent they are engaged in the performance of work for the Department, or utilize Department systems. IPC personnel must install and update anti-virus software on all computers maintained by the IPC, i.e., TEMPEST computers and non-TEMPEST classified computers within Controlled Access Areas (CAAs).

5 FAH-2 H-862 UNCLASSIFIED SYSTEMS

(TL:TEL-1;   07-01-1998)
(Uniform State/USAID/USIA)

a. DS/IST/ACD (Diplomatic Security, Information Security Technology, Assessment and Certification Division) authorizes systems personnel to update virus definition files from the anti-virus software vendor's Internet bulletin board or web-site via dial-up modem installed on an unclassified, stand-alone computer only. The computer may not be connected to or be a part of any LAN. The definition update files should be downloaded to a clean floppy diskette that contains no sensitive information. The standalone computer's hard drive must be scanned prior and subsequent to accessing the bulletin board or web-site. Scan the floppy diskette before use on any other USG computer. Use the clean floppy to copy the definition update files to all other unclassified computers.

b. At critical threat posts all software for use on unclassified systems within the CAA must be procured via secure channels. Downloading of virus definition update files for these systems is prohibited. Follow guidelines listed below.

5 FAH-2 H-863 CLASSIFIED SYSTEMS

(TL:TEL-1; 07-01-1998)
(Uniform State/USAID/USIA)

Downloading of updated virus definition files from the Internet or bulletin boards for classified systems is STRICTLY PROHIBITED. For all overseas posts, IRM/OPS/ITI/SI will send original program and updated anti-virus definition files via COMSEC channels in care of the COMSEC custodian in the diplomatic courier pouch. Make copies on properly procured diskettes. Do not use software copied from unclassified computers on classified computers.

5 FAH-2 H-864 INCIDENT REPORTING

(TL:TEL-1; 07-01-1998)
(Uniform State/USAID/USIA)

If a virus is discovered, send an official telegram or memorandum to the Department for IRM/OPS/ITI/SI/IIB and DS/IST/ACD. The report should include the following:

(1) name of virus and occurrences;

(2) location of virus (bureau, post or office);

(3) origin of virus infection;

(4) infected equipment type (stand-alone, LANs or network);

(5) type of software used to eradicate the virus;

(6) losses incurred (defined as loss of equipment, software or computer system downtime);

(7) point of contact for follow-up support; and

(8) remarks.

5 FAH-2 H-865 THROUGH H-869 UNASSIGNED